

MACHINE POLITICS

The man who started the hacker wars.

BY DAVID KUSHNER



In the summer of 2007, Apple released the iPhone, in an exclusive partnership with A.T. & T. George Hotz, a seventeen-year-old from Glen Rock, New Jersey, was a T-Mobile subscriber. He wanted an iPhone, but he also wanted to make calls using his existing network, so he decided to hack the phone.

Every hack poses the same basic challenge: how to make something function in a way for which it wasn't designed. In one respect, hacking is an act of hypnosis. As Hotz describes it, the secret is to figure out how to speak to the device, then persuade it to obey your wishes. After weeks of research with other hackers online, Hotz realized that, if he could make a chip inside

the phone think it had been erased, it was "like talking to a baby, and it's really easy to persuade a baby."

He used a Phillips-head eyeglass screwdriver to undo the two screws in the back of the phone. Then he slid a guitar pick around the tiny groove, and twisted free the shell with a snap. Eventually, he found his target: a square sliver of black plastic called a baseband processor, the chip that limited the carriers with which it could work. To get the baseband to listen to him, he had to override the commands it was getting from another part of the phone. He soldered a wire to the chip, held some voltage on it, and scrambled its code. The iPhone was now at his com-

mand. On his PC, he wrote a program that enabled the iPhone to work on any wireless carrier.

The next morning, Hotz stood in his parents' kitchen and hit "Record" on a video camera set up to face him. He had unruly curls and wispy chin stubble, and spoke with a Jersey accent. "Hi, everyone, I'm geohot," he said, referring to his online handle, then whisked an iPhone from his pocket. "This is the world's first unlocked iPhone."

Hotz's YouTube video received nearly two million views and made him the most famous hacker in the world. The media loved the story of the teen-age Jersey geek who beat Apple. Hotz announced that he was auctioning off the unlocked phone. The winning bid, from the C.E.O. of Cericell, a cell-phone-refurbishing company, was a 2007 Nissan 350Z sports car and three new iPhones. Later, on CNBC, Erin Burnett asked Hotz if he thought that day's uptick in Apple stock was due in part to his efforts. "More people want iPhones now if they can use them with any sort of provider," he said, and added that he "would love to have a talk right now with Steve Jobs" about it.

"Man to man?" Burnett said.

"Man to man."

Apple and A.T. & T. remained conspicuously silent. Unlocking a phone was legal, but it could enable piracy. Many hardware manufacturers sell the devices at a loss, recovering the costs through monthly contracts or software sales. When Steve Jobs was asked at a press conference about the unlocked iPhone, he smiled awkwardly and said, "This is a constant cat-and-mouse game that we play. . . . People will try to break in, and it's our job to keep them from breaking in." Hotz never heard directly from Jobs.

Steve Wozniak, the co-founder of Apple, who hacked telephone systems early in his career, sent Hotz a congratulatory e-mail. "It was like a story out of a movie of someone who solves an incredible mystery," Wozniak told me. "I understand the mind-set of a person who wants to do that, and I don't think of people like that as criminals. In fact, I think that misbehavior is very strongly correlated with and responsible for creative thought."

Hotz continued to "jailbreak," or unlock, subsequent versions of the iPhone until, two years later, he turned to his next

Radical hackers took up Hotz's fight, although he never considered himself a cause.

“It makes me
absurdly happy.”

—Peter Schjeldahl on “Selfless in the Bath of Lava,” at
MOMA PS1, from the new audio tour “Art in Queens”

The **GOINGS ON** app, a free guide to New York City culture from the staff of *The New Yorker*, features **audio tours** from some of the magazine's celebrated writers, along with a daily, digital version of the Goings On About Town listings section.

Download today at
newyorker.com/go/apps.

Available for Apple and Android mobile devices.



WINNER — AD AGE 2011 MEDIA VANGUARD AWARD
BEST CULTURE AND LISTINGS APP

Supported by



PRICELESS®
NEW YORK



Apple is a trademark of Apple Inc., registered in the U.S. and
other countries. App Store is a service mark of Apple Inc.
Condé Nast 2012.

target: one of the world's biggest entertainment companies, Sony. He wanted to conquer the purportedly impenetrable PlayStation 3 gaming console, the latest version of Sony's flagship system. "The PS3 has been on the market for over three years now, and it is yet to be hacked," he blogged on December 26, 2009. "It's time for that to change."

"My whole life is a hack," Hotz told me one afternoon last June, in Palo Alto, California. He had moved there the previous month. He was now twenty-one, stocky, and scruffy. He wore a gray T-shirt under a gray hoodie, ripped bluejeans, and brown suede moccasins. "I don't hack because of some ideology," he said. "I hack because I'm bored."

The word "hacker," when it was applied to technology, initially meant college students and hobbyists, exploring machines. At worst, a hacker was a prankster. In the early nineteen-seventies, Wozniak, the hacker archetype, built a system that let him make free phone calls. Among others, he called the Vatican, pretending to be Henry Kissinger, and managed to get a bishop on the line. Over time, "hacker" acquired a more sinister meaning: someone who steals your credit cards, or crashes the electronic grid. Today, there are two main types of hackers, and only one is causing this kind of trouble. A "white hat" hacker—an antivirus programmer, for instance, or someone employed in military cyberdefense—aims to make computers work better. It is the "black hat" hacker who sets out to attack, causing havoc or ripping people off. A recent series of attacks on Brazil's largest banks, which took down their Web sites for a short time, is an example of the malicious black-hat type. The number of black-hat intrusions is rising: in the U.S., the Department of Homeland Security has reported a spike—fifty thousand between October and March, up ten thousand from the same period last year.

Hotz likes to hack according to the early definition of the word: getting inside a machine to see how it works, and changing it. To him, hacking is almost a sport, played against someone in a position of authority. "It's a testosterone thing," he told me. "It's competitiveness, but it isn't necessarily competitiveness with other people. It's you versus the system. And I don't mean the system like the government

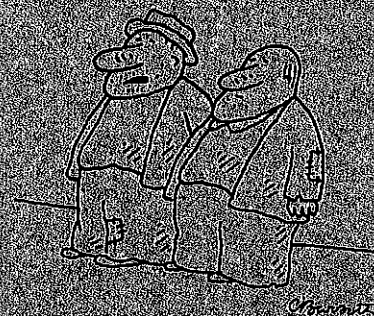
thing, I mean the system like the computer. I'm going to stick it to the computer. I'm going to make it do this! And the computer throws up an error like 'No, I'm not going to do this.' It's really a male thing to say, I'm going to make you do this!"

We were sitting in Hotz's apartment, on the ground floor of a building near Stanford. Red Bull cans and take-out menus littered the kitchen. Plastic wrappings, scattered cash, and empty computer boxes covered the living room. One box was overturned and being used as a dining table. A blue air mattress sagged in a corner. Hotz tossed a wad of cash from his pocket to the ground and sat with his legs crossed on a desk chair before three giant computer monitors. He held an iPad 2 that he had bought that afternoon at the Apple Store on University Avenue. Around the room, whiteboards were filled with scrawled notes and algorithms. One had a list labelled "Morning Routine": "7:15 a.m., one snooze? . . . shower . . . floss/brush/wash . . . vitamins . . . dress nicely . . . water plants." Another list, labelled "Uncomfortable Things," included "Call Therapist" and "Join Gym and Use It."

Hotz talked about how he wrote his first computer program when he was five, while sitting on his father's lap at their Apple II. By fifth grade, he was building his own video-game console with an electronic-projects kit from Radio Shack. His parents often found household appliances (remote controls, answering machines) gutted. "He always liked learning stuff, and if that was how he did it, great," his father, George Hotz, Sr., a high-school computer teacher, told me. Hotz, bored with his classes and letting his grades slide, became known at school as an inventive joker who rolled down the hallways in wheeled sneakers and once hacked several classroom computers to simultaneously play Beethoven's Ninth Symphony. His mother, Marie Minichello, a social worker, told me that although she punished him for his acts of mild disobedience, she always supported him. "I didn't want school to kill his passion," she said.

When Hotz was fourteen, he beat thousands of students from more than sixty countries to reach the finals of the Intel International Science and Engineering Fair. He appeared on the "Today" show with his invention, a small robot on wheels that could plot the dimensions of

Advertisement



"Good news—I hear the paradigm is shifting."

Talk to us.

Share your insights on a variety of topics with *The New Yorker's* marketing department as a member of our online Opinion Leaders panel. As one of our most influential readers, you'll gain VIP access to exclusive *New Yorker* events and special offers from our advertisers.

Sign up at

NewYorkerOpinionLeaders.com/Join

THE
NEW YORKER
OPINION LEADERS

Survey participation is 100% voluntary, and the information you provide will be kept strictly confidential.

© Condé Nast 2012

a room using infrared sensors, and wirelessly transmit the information to a computer. "Well, I think it's very cool to be good in science," Katie Couric told her viewers, as Hotz, in an ill-fitting dark suit, stepped forward, "and George Hotz is an example of that." Couric asked if the technology could improve automated vacuum cleaners. But Hotz was more excited about helping soldiers fight terrorists. "They can send it into a complex before the military infiltrates it!" he said, his voice not yet broken. "Well, I'm impressed, George," Couric replied, nudging him in the shoulder. "You're a little brainiac, you."

In high school, Hotz built the Neupilot, a sort of Segway controlled by brain waves, which you could drive around by thinking about it. Companies had explored similar technology for controlling video games, but building hardware controlled by brain waves still seemed like science fiction. The Neupilot worked, though the movements were not always precisely translated from the driver's brain. During his senior year, in 2007, Hotz built a "Star Trek"-inspired 3-D display called "I Want a Holodeck," which again made him a finalist at the International Science and Engineering Fair. This time, he topped the electrical- and mechanical-engineering category and won fifteen thousand dollars. Before a Forbes photo shoot for a story about his achievement, Hotz smoked pot for the first time. In the photograph, he told me,

smiling, "my eyes are bloodshot. It's great."

While he was talking, Hotz had been playing with the iPad 2. He planned to spend the night hacking it but needed computer cables. We drove to Fry's Home Electronics. It was around midnight, and as we approached a desolate intersection, hip-hop cranking from the car's sound system, the light changed to red. With an angry swerve of the wheel, he cut through an adjoining parking lot and kept driving, muttering, "Fuck these assholes. Stupidest red light ever. It makes no sense at all."

"I live by morals, I don't live by laws," he went on. "Laws are something made by assholes."

After high school, Hotz enrolled at the Rochester Institute of Technology but dropped out a few weeks later, to take up an internship at Google, in Silicon Valley. "We were not surprised or disappointed when he decided to leave school," his father told me, though he admitted that he sometimes worried about his son, who spent a lot of time alone. Hotz supported himself through donations from people who had downloaded software he'd written and given away free; one program let people jailbreak the iPhone 3GS. His hacks generated enough income that he was able to buy an old white Mercedes. But after a few months he grew bored at Google and in 2009 moved back home to New Jersey. Since his iPhone feat, geeks

often sent him devices just to see if he could hack them. That year, someone mailed Hotz a PlayStation 3 video-game system, challenging him to be the first in the world to crack it. Hotz posted his announcement online and once again set about finding the part of the system that he could manipulate into doing what he wanted. Hotz focussed on the "hypervisor," powerful software that controls what programs run on the machine.

To reach the hypervisor, he had to get past two chips called the Cell and the Cell Memory. He knew how he was going to scramble them: by connecting a wire to the memory and shooting it with pulses of voltage, just as he had when he hacked his iPhone. His parents often gave him gifts that were useful for his hobby: after he unlocked the iPhone, they bought him a more expensive one. For Christmas, 2009, they gave him a three-hundred-and-fifty-dollar soldering iron. Sitting on the floor of his room, Hotz twisted off the screws of the black PS3 and slid off the casing. After pressing the iron to the wire, he began pulsing the chips.

Next, he had to write an elaborate command that would allow him to take over the machine. Hotz spent long nights writing drafts of the program on his PC, and trying them out on the hypervisor. "The hypervisor was giving me shit," he recalls. It kept throwing up an error message—the number 5—telling Hotz that he was unauthorized. He knew that, if he got through, he'd see a zero instead. Finally, after several weeks typing at his computer, Hotz had composed a string of code five hundred lines long. He ran it on the PS3 and nervously watched the monitor. The machine displayed a sublime single digit: 0. Hotz called the code his "Finnegans Wake."

On January 23, 2010, a little more than a month after posting his challenge, Hotz announced on his blog, "I have hacked the PS3." He later posted instructions for others to do the same, and freely distributed the code. Hotz had hacked the two most iconic and ironclad devices of his generation. "Nothing is unhackable," he told the BBC. "I can now do whatever I want with the system. It's like I've got an awesome new power—I'm just not sure how to wield it."

Sony responded by releasing a software update that disabled OtherOS, the feature through which Hotz had ac-



"Nice, but as long as there are readers there will be scrolls."

cessed the hypervisor. OtherOS enabled the machine to run Linux, the alternative operating system to Microsoft Windows and Apple OS. Running Linux essentially turned the PS3 from a single-purpose gaming console into a desktop computer, which people could use to write programs. They were furious that Sony had robbed them of this capability. "I am EXTREMELY upset," a comment on Sony's blog read. Some wanted to rally around Hotz, and organize: "THIS IS MADNESS!!! HACKERS UNITE!!! GEOHOT WILL LEAD US INTO THE LIGHT!" But many were angry at Hotz, not at Sony. "Congratulations geohot, the asshole who sits at home doing nothing than ruining the experience for others," one post read. Someone posted Hotz's phone number online, and harassing calls ensued.

Recalling the controversy, Hotz seemed genuinely unfazed. "All those people flaming me, I could care less," he told me. He spent the summer of 2010 biking through China, and that fall, back at his parents' house, he read Ayn Rand, which he said made him want to "do something." "We let him get away with murder," his father admitted. "But he never did bad things. He always did what he felt was right, and we were happy with that."

In late December, Hotz decided once again to try to hack the PS3 in a way that would give him total control and let him restore what Sony had removed. On New Year's Eve, Hotz and some high-school buddies played beer pong and watched the Times Square ball drop on TV. He woke up hung over on the couch at a friend's house, with a towel stretched across him as a blanket, and stumbled back to his parents' to fix some macaroni and cheese and think things through. Hotz wanted control of the PS3 metldr (pronounced "met-loader"), a part of the software that, functioning like a master key, "lets you unlock everything."

Hotz knew that the metldr key was hidden within the PS3, but now he realized that he didn't necessarily have to find and break into the secret place. He could run a special decryption program in a different part of the machine, and make the key appear there. He had to figure out how to speak to the metldr, and then command it to appear. Within

ten minutes, he had coded the PS3 hack.

The cursor blinked, indicating that Hotz had the power to do anything with the PS3: install OtherOS, play pirated games, or run obscure Japanese software. He prepared a Web page and a video documenting what he had done. But he hesitated. Although Apple had never sued anyone for jailbreaking, Sony had reacted fiercely to previous modifications of the PlayStation. Sony had also long boasted about the security of the PS3. Hotz wasn't just undoing years of corporate P.R.; he was potentially opening the door to piracy.

With this concern in mind, Hotz wrote code that disabled the ability to run pirated software using his hack and added a note in his documentation: "I don't condone piracy." Still, he wanted a second opinion. Before he put the site live, he signed into an online chat channel where hacker friends hung out, and asked them whether he should release his hack. "Yeah," one told him. "Information should be free." Hotz told me, "This is the struggle of our generation, the struggle between control of information and freedom of information." Also, on the day of the hack, unbeknownst to his parents, Hotz was high. He told me he had taken Vicodin and OxyContin, which filled him with a sense of invulnerability. "You just feel good about everything," he recalled. He pushed a button on the keyboard and uploaded the instructions for his PS3 jailbreak.

On January 11, 2011, Hotz was playing Age of Empires II on his computer in New Jersey when he received an e-mail from Sony announcing a lawsuit against him. The company requested a temporary restraining order for violating the Computer Fraud and Abuse Act and facilitating copyright infringement, such as downloading pirated games. According to the Entertainment Software Association, piracy costs the industry eight billion dollars a year. Sony was also seeking to impound his "circumvention devices," and it wanted him to take all the instructions offline immediately.

As soon as the news hit the Web, geeks rushed to Hotz's site, seeking the tools while they could. At Carnegie Mellon University, David Touretzky, a computer scientist and proponent of freedom of information online, made copies of

ADVERTISEMENT

New Yorker Cover Prints

Find the one you love:
NewYorkerStore.com/Shop



Ilse Karasz, May 22, 1971



NewYorkerStore.com/Shop

Hotz's files. Touretzky blogged that Sony was "doing something breathtakingly stupid, presumably because they don't know any better. . . . Free speech (and free computing) rights exist only for those determined to exercise them. Trying to suppress those rights in the Internet age is like spitting in the wind." The Electronic Frontier Foundation, a digital-rights advocacy group, released a statement saying that the Sony v. Hotz case sent a "dangerous message" that Sony "has rights in the computer it sells you even after you buy it, and therefore can decide whether your tinkering with that computer is legal or not. We disagree. Once you buy a computer, it's yours."

But Sony believed that Hotz's hack was sending a dangerous message of its own. If people were free to break into their machines, game creators would be cheated out of royalties. Cheaters could tweak the games in order to beat everyone who stuck to the rules. Riley Russell, the general counsel for Sony Computer Entertainment of America, said in a statement at the time, "Our motivation for bringing this litigation was to protect our intellectual property and our consumers."

On January 14th, Hotz went on "Attack of the Show," a popular news program for gamers on G4, a cable-television network. When the host asked what he was being sued for, Hotz joked, "Making Sony mad." He was serious, though, about his mission to keep information free. Later, he uploaded a hip-hop video on YouTube, which he titled "The Light It Up Contest." He sat in front of his Webcam in a blue sweatshirt, his computer in the background. "Yo, it's geohot," he rapped, as the beat kicked in, "and for those that don't know, I'm getting sued by Sony." It was a surprisingly catchy tune about a complex issue from a whiz kid brazenly striking a pose. Hotz went on, bouncing in his desk chair, "But shit man / they're a corporation / and I'm a personification / of freedom for all."

Hotz's rap earned him sympathy in chat rooms but not in the courts. A California district court granted Sony the restraining order against Hotz, preventing him from hacking and disseminating more details about its machines. It also approved a request by Sony to subpoena information from Twitter, Google, YouTube, and Bluehost, Hotz's Internet provider, including the Internet Protocol

addresses of anyone who downloaded the instructions from his site—a move that further incensed digital-rights advocates. Sony also gained access to records from Hotz's PayPal account. In some circles, the rebel leader was becoming a martyr. As one fan of Hotz's posted: "geohot = savior of mankind."

Martyrs win devotees, and soon Hotz had gained the allegiance of the most notorious hackers: a group called Anonymous. In the past few years, the group has become famous for engineering elaborate online attacks and protests, often in the name of free speech and "lulz," which is Internet-speak for laughs. Group members fought against the Church of Scientology, which they believed to be suppressing free speech online, and shut down government Web sites in defense of WikiLeaks. More recently, coders have joined the Occupy Wall Street movement, and threatened to release a list of people collaborating with the Zetas, a Mexican drug gang. At the time of the Sony hack, Anonymous had become its own pop-culture meme. On Comedy Central, Stephen Colbert called Anonymous members a "global hacker nerd brigade." Others referred to them as "the paramilitary wing of the Internet."

Anonymous is an international, decentralized, shape-shifting hive. All you have to do to join is say you are part of it. No one goes by his or her real name. As in any shadowy group, some members are more extreme than others. A few years ago, I was invited to attend a secret meeting of Anonymous activists, at an Indian restaurant in Hollywood. While Anonymous is often characterized as a group of malicious cyber-terrorists, they struck me more as a group of earnest young protesters with a dark sense of humor and a brilliant knack for viral marketing. Anons, as members call themselves, are the best publicists on the Internet: through social media, they mobilize, inform, outrage, and entertain in

ways that the Yippies could never imagine, and they do it all really fast."

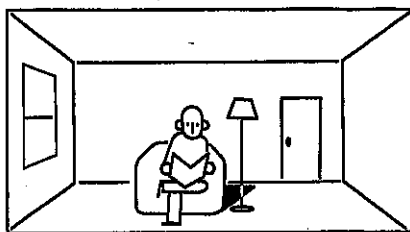
In early April, an Anonymous member created an Internet relay chat room called Operation Sony, or #OpSony. "It is the duty of Anonymous to help out this young lad, and to protest against Sony's censorship," the mission statement read. Around the world, curious coders logged into their phones and laptops to discuss plans.

As the chat room filled, Anons began digging up personal contact information on Sony's lawyers and debating the most effective tactics: Flash mobs outside Sony stores? Sending black faxes, which would waste all the ink in their machines? Eventually, they settled on a distributed denial of service, or DDoS, attack, overwhelming Sony's Web sites with simultaneous visits until they crashed.

On April 4th, Anonymous announced the plan to the public in a press release: "Congratulations, Sony. You have now received the undivided attention of Anonymous. You saw a hornets nest, and stuck your penises in it. You must face the consequences of your actions, Anonymous style." Within hours, both Sony.com and PlayStation.com were down. Anonymous posted a video on YouTube with its demands: Drop the case against Hotz and allow for modifications on the PS3. Over an image of a Guy Fawkes mask, which the group uses as a symbol, text read, "Leave Fellow hackers like geohot alone."

Internet protests, like street protests, have a way of spinning out of control. People chant peacefully, but then someone throws a rock through a window and rioting begins. No sooner had the hacker war begun than one Anon declared a splinter faction, SonyRecon, calling for personal hacks against Sony employees and the judge in the geohot case. Other Anons posted the phone numbers, family-member names, and addresses of Sony executives. They even published a description of the C.E.O.'s house, and proposed various methods of attack:

<sonyrecon335> We'll shit on his doorstep, then run away
<e-hippie741> dude
<e-hippie741> you'd shit on someones doorstep
<Hit_X> ring the kids school and pull a prank like hes been rushed in hospital:
<e-hippie741> do you love geohot that much

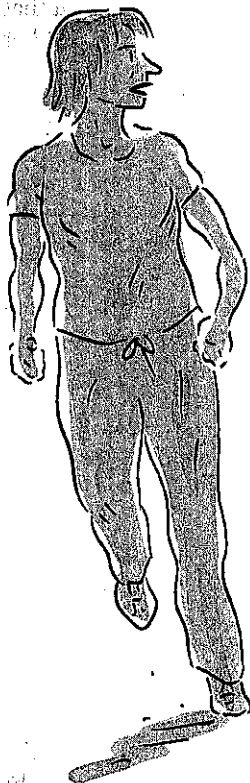


Back in his parents' house, in front of the glowing computer screens in his cluttered bedroom, Hotz clicked with mounting apprehension through the news of Anonymous's plans. "I hope to God Sony doesn't think this is me," he remembers thinking. He didn't believe in secretive online warfare, much less in defecating on someone's doorstep. "I'm the complete opposite of Anonymous," he told me. "I'm George Hotz. Everything I do is aboveboard, everything I do is legit."

On April 11th, Sony announced that it had reached an agreement with Hotz, who denied wrongdoing but consented to a permanent injunction barring him from reverse-engineering any Sony product in the future. But Hotz's supporters felt that the injunction was a form of censorship. Some of his defenders made "FREE GEOHOT" shirts, and others went to Sony stores in cities such as San Diego and Costa Mesa to protest. Black-hat hackers called for more destructive attacks against Sony.

At 4:15 P.M. on April 19, 2011, technicians at the San Diego offices of Sony Network Entertainment noticed that four of their computer servers were rebooting without authorization. The team took the systems offline and began examining the activity logs. Their investigation confirmed that someone had broken into the servers, and possibly into others. Sony immediately shut down the PlayStation Network, their online-entertainment hub. The company concluded that it had been the victim of a sophisticated attack that had exposed the addresses, passwords, birthdays, and e-mail addresses of seventy-seven million PSN subscribers, who pay to play games and watch movies. "While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility," Patrick Seybold, a company spokesman, wrote in a blog post on PlayStation's Web site. Though it remained unclear whether someone from Anonymous was responsible for the hack or whether it was just someone taking advantage of the chaos, the events were clearly linked.

Security experts called it one of the biggest data breaches of all time. Sony announced that it would keep the PSN down indefinitely—at an estimated cost



WARY

"I'm thinking about letting myself get old."

of ten million dollars in lost revenue per week—as it raced to plug the holes. Anonymous denied responsibility and temporarily suspended its campaign against the company.

At 4:51 A.M. on April 28th, Hotz uploaded a lengthy rant against the PSN hackers. "Running homebrew and exploring security on your devices is cool," he wrote. "Hacking into someone else's server and stealing databases of user info is not cool. You make the hacking community look bad, even if it is aimed at douches like Sony." Hotz was pointing out the distinction between white- and black-hat hackers. Still, he knew he had helped loosen a boulder that was now crashing down a hill.

On May 1st, the company discovered a data breach on the Sony Online Entertainment service, exposing twenty-four million personal accounts. Technicians also found a file that had been planted on one of their servers as a kind of digital graffiti. It was titled "Anonymous," and read, "We Are Legion." At a press conference in Tokyo that day,

Kaz Hirai, the chief executive officer of Sony Computer Entertainment, and two other executives walked onto a stage and faced the packed crowd. "We offer our sincerest apologies," Hirai said and, setting his microphone on a table, bowed low with the others for eight seconds as the cameras flashed. They said that some network services would be back up in a few days. But it took two weeks to fully restore the system.

Sony soon had a new force to contend with: an Anonymous splinter group called Lulz Security, commonly known as LulzSec. Members were like the merry droogs of the net; on their Twitter feed, nicknamed the Lulz Boat, they identified themselves as "the world's leaders in high-quality entertainment at your expense." Their first bit of dark comedy came on May 30th, when they hacked the PBS Web site, in retaliation for what they thought was unfairly negative coverage of the WikiLeaks founder, Julian Assange. They posted a fake news story reporting that the late rappers Tupac Shakur and Biggie Smalls had been hiding out in New

Zealand. "Local townsfolk refuse to comment on exactly how long or why the rappers were being sheltered," the story read. "One man simply says 'we don't talk about that here.'"

The day after the PBS prank, the group began tweeting a series of warnings to Sony. "Hey @Sony," one read, "you know we're making off with a bunch of your internal stuff right now and you haven't even noticed? Slow and steady, guys." Some saw the warnings as more geohot backlash for the company. "The group is sending a message to Sony for messing with one of their own, hacker George Hotz," a blogger wrote.

On June 2nd, LulzSec hacked the Sony Pictures Web site, compromising what it claimed to be more than a million passwords of consumers who had put their personal information on the site. (Sony later put the figure at thirty-seven thousand.) The group's purpose, it explained in a statement, was not to come across as "master hackers" but to expose the continued weakness of Sony's security systems. Lulz's statement said that Sony was "asking for it," because the company stored the passwords in plain text, instead of encrypting them. The statement went on to encourage fellow-hackers to "tear the living shit out of it while you can; take from them everything!" LulzSec members broke in using a rudimentary technique called SQL Injection, which allowed them access to unauthorized data on the Sony Pictures site. "From a single injection, we accessed EVERYTHING," they said. "Why do you put such faith in a company that allows itself to become open to these simple attacks?"

Black-hat hackers began posting corporate e-mails, and, during the summer of 2011, attacks on media, technology, and other institutions came almost daily. Nintendo got hacked, and so did Sega, Electronic Arts, the News Corporation, Booz Allen Hamilton, NATO, and Lady Gaga. Even the C.I.A. was hacked, LulzSec claimed. It was the Summer of Lulz. Hotz didn't mean to inspire a hacker war, but he doesn't regret what he did. One night at a restaurant in Palo Alto, he clarified his position on the attacks against Sony. "If being a techno-libertarian leads to online anarchy, so be it," he said. "I'm not a cause. I just like messing with shit."

Hotz defines a hacker as "somebody with a set of skills," and points out that the skills alone don't make you good or evil. It's up to you to decide how to use them. Facebook's Mark Zuckerberg may be his generation's most famous hacker, but Hotz most embodies its original spirit. He hacks for the technical challenge and the fun. He doesn't identify as white-hat or black-hat, preferring to think of himself more like someone twisting wrenches under a sink. "Hacker is to computer as plumber is to pipes," he once blogged. When I met him again, later in the summer, at DefCon, a hacker convention in Las Vegas, he wasn't at a bar with guys in long black coats, plotting some corporate takedown. He was alone on a couch in a back room, coding on his laptop.

A month after his settlement with Sony, last spring, Hotz moved back to California to take a full-time job at Facebook. He wouldn't say what he worked on, other than design technology to improve the site. Some saw his transition as a shrewd move by Facebook to co-opt a hacker before he might compromise the company. Others flamed him for cashing in. "You have to love the amount of suck and sell-out that George Hotz contains within his flimsy nerd shell," a detractor wrote online.

One of my interviews with Hotz took place in Palo Alto just after he'd started the Facebook job, before word had leaked online. He showed up wearing a new blue-and-white Facebook T-shirt, a member of the Valley's coolest frat. He was waking up early (as his "Morning Routine" whiteboard reminded him) to get to work. "Everything is very fast-moving and the culture is young," he said, and then handed me his business card, which read, "I am the most illegal circumvention device of them all." Eight months later, Hotz quit. He didn't want to discuss why, but suggested that having a day job didn't suit him. "Facebook is a fun place to work," he told me, "but I wonder how people stay employed for so long." He travelled in Panama, then returned to Palo Alto. He wouldn't say what he was going to do next, only that he won't be sharing his exploits on the Internet anymore. "I'm through with all that," he said.

He wasn't the only one. On March 6, 2012, U.S. officials announced the indictment of six elite hackers from Anonymous and LulzSec. A federal law-enforcement official told me that the arrests were "very significant—these are core members." Hotz had never made contact with LulzSec or Anonymous members, even when they were crusading on his behalf, and he was agnostic about their fate. The brash young man from the rap video who described himself as "a personification of freedom for all" had retired from battle. He refused to make what he called "a moral judgment" of the indicted hackers. "I'll make a technical judgment," he told me. "If they were that good, they wouldn't have got caught."

Even with the arrests, other Anons have sworn to keep up the campaign. Companies are working hard, too. "The last year has demonstrated how sophisticated cybercriminals can be," Jim Kennedy, the senior vice-president of strategic communications for Sony Corporation of America, wrote me in an e-mail. Sony created a new position—a corporate executive in charge of global-information security and privacy—and promoted Nicole Seligman, who as general counsel had been targeted by hackers, to president of the Sony Corporation of America. Kennedy admits that security remains an unceasing fight. "In the end, it must be recognized that no system is absolutely foolproof," he wrote. "Constant vigilance is essential."

Last May, engineers from Sony invited Hotz to a meeting at its American headquarters, a half hour's drive north, in Foster City. ("We are always interested in exploring all avenues to better safeguard our systems and protect consumers," Kennedy told me.) Nervous but curious, Hotz walked into the building eating from a box of Lucky Charms, dropping marshmallows across the lobby. "If there were going to be lawyers there," he recalled, "I was going to be the biggest asshole ever." Instead, he found a roomful of PS3 engineers who were "respectful," he said, and wanted to learn more about how he had beaten their system. During the next hour or so, the man who had started the hacker wars described his methodology. ♦

NEWYORKER.COM/GO/ASK

David Kushner takes readers' questions.